aefinfo.fr

L'opération Cactus de sensibilisation des élèves aux cyberattaques est étendue à toutes les académies

Emmanuel Fontaine

7–9 minutes

La nouvelle campagne de sensibilisation aux cyberattaques a été lancée le 19 mars dans toutes les académies auprès de plus de 2,5 millions d'élèves, à travers un message frauduleux déposé sur leur ENT. Si 210 000 d'entre eux ont mordu à l'hameçon, il s'agissait de "mettre les élèves en situation eux-mêmes d'être piégés", selon Johanna Brousse, chef de la section de lutte contre la cybercriminalité au parquet de Paris. Il était question de susciter les débats et de "parler de cybersécurité sous un angle nouveau", pour le directeur général de cybermalveillance.gouv.fr Jérôme Notin.

La nouvelle campagne de sensibilisation aux cyberattaques a été lancée le 19 mars dans toutes les académies. ShutterStock

"Nous sommes persuadés que la prévention est essentielle pour éviter aux jeunes de passer par la case prison", assure lundi 24 mars 2025 la vice-procureure et cheffe de la section de lutte contre la cybercriminalité (Junalco) au parquet de Paris Johanna Brousse, lors d'un retour d'expérience sur la nouvelle opération de sensibilisation des élèves du second degré aux cyberattaques.

Mettre les élèves "en position de victimes"

En 2024, face à la recrudescence de mineurs impliqués dans des cyberattaques, et notamment le piratage de plusieurs Espaces numériques de travail (ENT) ayant entraîné l'ouverture d'enquêtes et d'instructions, la Junalco lance un groupe de travail autour du ministère de l'Éducation nationale, du ministère de l'Intérieur (Comcyber-MI ([lire sur AEF

info)), de la Cnil et de cybermalveillance.gouv.fr (GIP Acyma) pour mener des actions de sensibilisation.

Pour être "efficace", l'action "doit mettre les élèves en situation eux-mêmes d'être piégés", explique Johanna Brousse. Elle consiste à l'envoi de mails de "hameçonnage" aux élèves via les ENT pour qu'ils "soient mis en position de victimes et qu'ils se rendent comptent que les cyberattaques ne sont pas irréelles et peuvent concerner tout le monde". De plus, poursuit-elle, "des réunions que nous avons eues avec Interpol ont montré des situations de pays très impliqués à l'étranger, comme aux Pays-Bas", qui portaient ces opérations à "fort impact".

L'opération Cactus 2

Après avoir été testée dans sept départements (les Yvelines et les six départements de l'académie d'Orléans-Tours), l'opération Cactus a donc été reconduite en 2025 avec un "passage à l'échelle", c'est-à-dire en la proposant à toutes les académies.

Cependant, "comme les académies ont toutes des organisations différentes pour leurs ENT, explique Stéphane Guérault, qui a piloté le dispositif pour l'Éducation nationale, "nous leur avons laissé le choix de la stratégie de déploiement". Par exemple, tous les collèges et lycées de la région Grand-Est ont été concernés, tandis que ce fut uniquement le cas des 4e et des secondes à Mayotte.

La stratégie a donc consisté à envoyer un message d'hameçonnage mercredi 19 mars 2025, via un compte fictif créé pour l'occasion, à quelque 2,5 millions d'élèves. Résultat, 210 000 élèves ont cliqué sur le lien indésirable, soit environ 8 %, alors que le taux était de 13 % lors du test de l'année précédente. Si ces élèves sont tombés dans le panneau, le directeur général de cybermalveillance.gouv.fr Jérôme Notin trouve l'opération vertueuse, du fait que la vidéo de prévention sur laquelle ils étaient renvoyés a été vue 135 000 fois.

Une capture d'écran d'un exemple de fishing envoyé à des élèves sur leur ENT pourl'opération Cactus de 2025.

| *AEFinfo*

Le lendemain de la fausse "cyberattaque", des affiches ont été déployées dans les établissements pour "lancer les débats" sur cette thématique, avant qu'un message ne soit envoyé aux parents d'élèves pour expliquer l'opération.

En parallèle, un kit de sensibilisation a été fourni pour les enseignants souhaitant réaliser un atelier de 50 minutes sur le sujet.

Il comporte trois fichiers :

- un guide avec détail de la séance ;

- une fiche élève à compléter et corriger ;
- une présentation PowerPoint pour permettre de s'emparer de la séance.

Se protéger c'est aussi protéger les autres

Au final, pour Jérôme Notin il s'agissait avant tout de réussir à "parler de cybersécurité sous un angle nouveau". Interrogés à la suite de cette expérience, 600 établissements sur les 4 700 concernés (soit 13 %) ont exprimé leur ressenti. Parmi eux, 70 établissements se sont engagés à déployer une action d'ici aux prochaines vacances scolaires, dont la moitié via les professeurs principaux. Dans un quart d'entre eux des débats ont été initiés par les équipes éducatives. "Ce qui a été intéressant c'est également le test de la chaîne d'alerte : dans 50 % de ces établissements, un signalement a été constaté", plaide-t-il.

Xavier Delporte, directeur des relations avec les publics de la Cnil, se félicite de cette "opération collective de politiques publiques qui se mobilisent sur cet enjeu majeur", d'autant que les jeunes "sont particulièrement exposés à ces menaces cyber".

Car s'ils sont très connectés et nés avec le numérique, les jeunes peuvent "avoir tendance à ne pas être assez attentifs", tandis que l'entourage familial "n'a pas toujours la possibilité de les accompagner".

un travail "collectif" pour faire diminuer la menace du vol et du partage de données personnelles

D'où le rôle fondamental de l'école mais aussi, d'un travail "collectif" pour faire diminuer la menace du vol et du partage de données personnelles non souhaitées, estime à son tour Guillaume Deckmyn, chef du département stratégie cyber au ministère de l'Intérieur.

Cette nouvelle opération s'inscrit en effet "dans la stratégie globale de lutte contre la cybercriminalité". Elle consiste à "fournir des armes" pour aider les jeunes à devenir ambassadeur cyber, "permettre de réduire le risque" que fait porter sur la société la future menace cyber, et enfin de "contribuer à faire émerger une culture de la cybersécurité".

D'autres opérations "Cactus", directement gérées par les académies, se dérouleront dès la fin de l'année.

Quel ressenti pour les élèves ?

Préparation du programme de sensibilisation aux cyberattaques, au lycée Montaigne à

Paris le 19 mars 2025.

| *AEFinfo*

Pour "avoir un ressenti" sur le dispositif, des interventions sur le terrain ont également eu lieu dans plusieurs établissements scolaires la semaine du 17 mars 2025. AEF info a assisté à un atelier au lycée Montaigne à Paris, mené par le lieutenant-colonel Sophie Lambert.

Durant une heure, le lieutenant s'est adressé à des élèves de seconde pour leur faire comprendre que "les ENT paraissent totalement sécurisées, mais les hackers trouvent des failles". À travers des exercices, le but était de leur faire comprendre la façon dont fonctionne le hameçonnage ou les infostealers : "les poissons c'est vous, et le hacker il attend", fait valoir Sophie Lambert.

Parmi les messages transmis aux élèves, l'importance de prendre son temps avant de cliquer sur un lien, de surveiller ses connexions réseau, ou encore les signaux d'alerte à décrypter lors de la réception d'un mail.